Spring 2007

Trust Not Their Presents, Nor Admit the Horse: Countering the Technically-Based Espionage Threat

Robert Gray Bracknell

U.S. Marine Corps

Follow this and additional works at: http://docs.rwu.edu/rwu_LR

Recommended Citation
Available at: http://docs.rwu.edu/rwu_LR/vol12/iss3/6
Trust Not Their Presents, Nor Admit the Horse: Countering the Technically-Based Espionage Threat

Robert Gray Bracknell*

O wretched countrymen! what fury reigns?
What more than madness has possess'd your brains?
Think you the Grecians from your coasts are gone?
And are Ulysses' arts no better known?
This hollow fabric either must inclose,
Within its blind recess, our secret foes;
Or 't is an engine rais'd above the town,
T' o'erlook the walls, and then to batter down.
Somewhat is sure design'd, by fraud or force:
Trust not their presents, nor admit the horse.

Virgil, The Aeneid
Book II, Section 1

* Robert Gray Bracknell is an active duty Major in the U.S. Marine Corps, currently serving as the Aide de Camp to the Commander, U.S. Marine Corps Forces Command, Norfolk, Virginia. He is a 1992 graduate of the University of North Carolina (B.A.), a 1999 graduate of the University of Maryland School of Law (J.D. with honors), and a 2006 graduate of Harvard Law School (LL.M.). Major Bracknell's service includes duty as an armor officer (M1A1 Abrams tanks) at 2nd Tank Battalion, 2nd Marine Division; as a Joint Task Force-160 infantry platoon commander and assistant operations officer in Guantanamo Bay, Cuba; as a military prosecutor and Special Assistant U.S. Attorney; as an assistant legal advisor at Headquarters, NATO Stabilization Force, Sarajevo, Bosnia and Herzegovina and Headquarters, U.S. European Command, Stuttgart, Germany; and as the principal legal advisor at U.S. Marine Corps Forces, Europe, Stuttgart Germany and 3d Marine Aircraft Wing (Forward), Al Asad, Iraq. He resides with his wife Rebecca and three children, Reagan, Jackson, and Quinn, in Virginia Beach, Virginia.

1. VIRGIL, THE AENEID OF VIRGIL 25 (J.W. Mackail, M.A. trans., 1885). Virgil's epic The Aeneid chronicles the story of the Trojan hero and founder of Rome Aeneas, who escaped Troy with his father and son after the city was
I. INTRODUCTION

States spy on one another, because all states want to know what the other ones are up to. The trick, then, is to be effective with your own spying, while limiting the effect of the other states’ spying. This Article seeks to offer policy recommendations regarding a specific subset of this epic problem: countering the espionage of foreign powers – states, particularly China; non-state actors, including organized crime syndicates and transnational terrorists; and ordinarily legitimate business organizations – through technical means, such as compromising U.S. information systems through hacking, electronic surveillance of U.S. information assistance, and cyberattack. Fourteenth century Chinese war philosopher Sun Tzu’s offers pithy observations regarding espionage and spycraft:

All warfare is based on deception. There is no place where espionage is not used. ... Be extremely subtle, even to the point of formlessness. Be extremely mysterious, even to the point of soundlessness. Thereby you can be the director of the opponent’s fate. ... A military operation involves deception. Even though you are competent, appear to be incompetent. Though effective, appear to be ineffective.

Bearing in mind that Sun Tzu’s philosophy may pervade Chinese strategic planning, and certainly influences U.S. planning, the

sacked by the Greeks. The Greek army was led by Ulysses, using the legendary Trojan horse to effect clandestine entry to the walled city. The Trojans were routed. See generally id.

2. For the purposes of this paper, I concentrate specifically on China as an emerging state-based rival with an active espionage/counterintelligence program. Such concentration should not be interpreted to exclude consideration of other state rivals or competitors, such as Russia, France, Iran, India, Japan, North Korea, South Korea, Taiwan, Israel, or any one of another dozen states or non-state actors with varying degrees of technical espionage capacity.

3. SUN Tzu (CHINESE GENERAL AND STRATEGIST), THE ART OF WAR (circa 400 B.C.).

4. See, e.g., China’s Strategic Intentions and Goals: Hearing Before the H. Comm. on Armed Services, 106th Cong. (2000) 14, 17-18 (testimony of Larry M. Wortzel, Director, Asian Studies Center, The Heritage Foundation) (Beijing has turned one of the maxims of Sunzi (or Sun-tsu, author of The Art of War), into a twenty-first-century security strategy. China is “attacking the
U.S. must be specifically concerned regarding the presence of a subtle, soundless and formless Chinese threat lurking to collect information that would direct the U.S. fate in the budding interstate competition.

The People's Republic of China is emerging as the possible leading state-based rival of the U.S. for the twenty-first century,\(^5\) the way that the Soviet Union, and, to a lesser extent, the Third Reich and Imperial Japan served as state-based strategic opponents in the last century, and Great Britain in the early part of the century prior. It stands to reason, then, that the U.S. would seek to gain and maintain an information advantage with regard to China – we want to know what they are doing, planning, and thinking, while denying them access to the same information pertaining to the U.S. Chinese military philosopher Sun Tzu's sublime aphorisms regarding espionage, deception, and information security are apropos counsel for assessing the Chinese approach, and defining U.S. policy on this issue. I seek to define the problem of technically-based espionage; identify methods and techniques that foreign powers employ to realize espionage activities; propose legally-based avenues of attacking the problem through detection and deterrence; and make recommendations on any necessary legislative reform required to leverage a well-

---

positioned commercial enterprise to effect a more robust defense against technically-based espionage. Espionage is a threat to the security and prosperity of the United States, a nation of laws – so we ought to be able to use law as a tool to detect it, deter it, and attack it.6

II. DEFINING AND FRAMING THE ISSUES

On January 19, 2002, The Washington Post broke a story regarding purported U.S. attempts to spy on China.7 The Chinese government had recently purchased a Boeing 767-300ER jetliner for use as Chinese President Jiang Zemin’s official state aircraft.8 Presumably during security sweeps by Chinese counterintelligence personnel, the aircraft was discovered to have contained around two dozen surveillance and listening devices embedded throughout the plane,9 including in Zemin’s bedroom. The aircraft had been customized in San Antonio, Texas by four subcontractors for President Zemin’s use.10 It is uncertain as to exactly when the listening devices were inserted, or even whether U.S. intelligence agencies were, in fact, responsible for the installation of the surveillance gadgets11 – though it is a fair

6. The use of law and legal processes offensively or in a proactive defensive manner has been termed “lawfare” by some forward-leaning commentators. See Lawfare, the Latest in Asymmetries (Transcript of FY03 National Security Roundtable), COUNCIL ON FOREIGN RELATIONS, Mar. 18, 2003, http://www.cfr.org/publication.html?id=5772 (“Lawfare is a strategy of using or misusing law as a substitute for traditional military means to achieve military objectives.”)


10. See Pomfret, supra note 7, at A1.

assumption that the intelligence community was attempting espionage by placing tireless, soundless, virtually formless electronic spies inside Zemin's aircraft. Ultimately, whether the U.S. was responsible for this attempted espionage is immaterial to raising the issue that the aircraft bugging could have been the implementation of a foreign intelligence gathering technique.12

If U.S. intelligence agencies sponsored the technical modification of the airplane before it was exported to China, why then might the Chinese, or some other foreign power, not seek to plant similar information-gathering technologies — technical devices or software which capture data and transmit it through the internet to other information systems designed to receive and cache the data13 — into host products exported to the U.S.? It is well known that the Chinese government sponsors web and internet-based attacks on Western information infrastructures, attempting to find gaps in information security defenses in order to exploit information.14 As FBI Director Robert Mueller noted in

12. See Cao Xueyi, The Wolf Has Come, PLA DAILY (MEDIA PRODUCT OF THE CHINESE PEOPLE'S LIBERATION ARMY), Aug. 25, 1999, at 5, available at http://www.usembassy-china.org.cn/sandt/secwolf.html (recognizing the potential for Chinese information system security breaches: "[E]ighty percent of computer security problems are caused by management errors. Computer spies take advantage of these errors. They use electromagnetic sensors, bugs, or advanced network equipment to monitor a computer's CPU, peripherals, terminals, communications equipment and network information. Making use of electromagnetic reflections, information and images on a computer system can be captured remotely using appropriate electronic equipment. Using various direct and indirect pathways, they enter Chinese military computer systems, steal information and damage systems or use computer viruses to change computer data. This can affect the entire computer system and cause a failure.").


testimony before the U.S. Senate Select Committee on Intelligence,

The cyber-threat to the U.S. is serious and continues to expand rapidly the number of actors with both the ability and the desire to utilize computers for illegal and harmful purposes rises.

Cyber threats stems from both state actors, including foreign governments that use their vast resources to develop cyber technologies with which to attack our networks, and non-state actors such as terrorist groups and hackers that act independently of foreign governments. The increasing number of foreign governments and non-state actors exploiting U.S. computer networks is a major concern to the FBI and the Intelligence Community as a whole.

State actors continue to be a threat to both our national security as well as our economic security because they have the technical and financial resources to support advanced network exploitation and attack. The greatest cyber threat is posed by countries that continue to openly conduct computer network attacks and exploitations on American systems.¹⁵

Moreover, the recent acquisition by Chinese computer manufacturer Lenovo of IBM’s personal computer division¹⁶ has

---


¹⁶. See Steve Lohr, Is I.B.M.’s Lenovo Proposal a Threat to National Security?, N.Y. TIMES, Jan. 31, 2005, at C6 ("Most I.B.M. personal computers are now produced in China. Like other PC’s, the I.B.M. machines are powered by Intel microprocessors and are assembled with chips and parts made
given rise to suspicion within the U.S. Obviously, some foreign-made and foreign-modified information technology products, including hardware and software, make their way into the U.S. stream of commerce, including to U.S. government use, particularly by the military, the Departments of Defense and State, other departments and agencies, the intelligence agencies themselves, the Executive Office of the President, and Congress. The scenarios of concern are:

- That a foreign manufacturer is infiltrated around the world, though mainly in East Asia. ...

17. Chinese Computer Maker Is Open To Inquiry on Sale to State Department, N.Y. TIMES, Mar. 25, 2006, at C2; Keith Bradsher, State Department is Criticized for Purchasing Chinese PCs, N.Y. TIMES, Mar. 24, 2006, at C5; Lenovo Under U.S. Probe for Spying, SLASHDOT.ORG, Mar. 30, 2006, http://it.slashdot.org/article.pl?sid=06/03/30/1344211 ("Lenovo, the giant Chinese PC manufacturer, is under a probe by the U.S.-China Economic Security Review Commission (USCC) for possible bugging. Apparently, the [U.S.] government has ordered 16,000 PCs from Lenovo but is now requesting that Lenovo be investigated by intelligence agencies. The fear is of foreign intelligence applying pressure to Lenovo to equip its PCs so that the U.S. can be spied on. ... 'Despite the probe, Lenovo says that its international business, especially those that deal with the U.S., follow strictly laid out government regulations and rules. Lenovo also claims that even after purchasing IBM's PC division, its international business has not been affected negatively. Interestingly, in an interview with the BBC, Lenovo mentioned that an open investigation or probe may negatively affect the way that the company deals with future government contracts or bids.'").

18. See Joseph Kahn, Chinese Leader Focuses on Business as 4-Day U.S. Visit Begins in Washington State, N.Y. TIMES, Apr. 19, 2006, at A8 ("Microsoft, which gave [current Chinese President Hu Jintao] a tour of a hyper-technological home of the future, was reaping the rewards of a new regulation requiring all Chinese-made computers to preinstall a copyrighted operating system to prevent piracy.

In the past two weeks, Microsoft has signed four agreements with Chinese computer manufacturers to preinstall Windows. The largest came Monday, when [Chinese government-owned] Lenovo Group said it would spend $1.2 billion over the next year on Windows."). The potential for Chinese modification of the Windows program for economic and security-related espionage purposes is apparent.
unknowingly by agents of a foreign power, who insert, undetected, microhardware or undetectable computer code into products destined for U.S. markets and U.S. government purchase and use;

- A foreign manufacturer is deliberately complicit in the same scheme;
- A U.S. domestic company is infiltrated or willfully complicit in such a scheme;
- A U.S. company, or a controlling interest in a U.S. company, is acquired by a foreign entity and its manufacturing, assembly and distribution processes are corrupted by the foreign entity; or,
- A U.S. domestic company unknowingly integrates adulterated components manufactured or assembled abroad into a product destined for U.S. government purchase and use.

“Buy American” is an obvious, yet wholly unworkable, solution: in the era of integrated economies, particularly in information systems, it is virtually impossible for a U.S. manufacturer to use only wholly domestic components in its final product\(^\text{19}\) – not to mention the practically unavoidable WTO proceedings alleging protectionism that would follow – and even then, infiltration by foreign agents posing as researchers or technical workers presents a continuing vulnerability. For example, the virtually ubiquitous Blackberry communications device is manufactured by Research in Motion, Inc.,\(^\text{20}\) in Waterloo, Ontario, Canada,\(^\text{21}\) and Amkor Technology, Incorporated, a Chandler, Arizona corporation producing components for cell phones, personal computers, and other products,\(^\text{22}\) has major

\(^{19}\) See generally David G. McKendrick, Richard F. Doner, & Stephan Haggard, From Silicon Valley to Singapore: Location and Competitive Advantage in the Hard Disk Drive Industry (2000).


manufacturing facilities in Pudong, Shanghai, China. Intel, Inc., a leading manufacturer of computer chips, motherboards, and other information system components integrated into the products of virtually every major information systems manufacturer, has employees in 45 countries, manufacturing facilities in China and Malaysia and research and development facilities in Russia, and performs a "substantial majority" of component assembly and testing in Costa Rica, China, Malaysia, and the Philippines. Avoiding foreign technology is simply not possible in the integrated world economy.

By borrowing from the American legal concept of products liability, in which the burden of designing harmless products and bearing risk regarding to the safety of a product’s design and manufacture is shifted onto companies rather than consumers, the law can impose special duties on companies engaged in information technology commerce aimed at U.S. consumers, including the U.S. government, and can require them to take prudent steps mandated by law to ensure that the products they sell are as “espionage-safe” as possible. Companies engaged in the enterprises of manufacturing, assembling, and distributing information systems components simply are in a better position than the U.S. government or other end users to prevent the adulteration of their products. First, companies can use trusted agents to verify the quality control of their products to ensure no espionage-enabling parasitic technology is emplaced. Moreover, companies have a knowledge advantage regarding the engineering

and production processes of their own products.

In short, companies can be economically incentivized, through legal sanction, to take prudent steps to ensure that products sold to the U.S. government and entering the stream of U.S. commerce are "espionage-safe." The burden should fall on the party on whose "watch" the vulnerability is introduced; that is, if a company allows, deliberately or negligently, a monitoring or surveillance device to be engrafted onto its product, why should the burden of discovery lie with the customer? Such a construct is as inconsistent with basic notions of commercial fairness as requiring a homeowner who purchases a new lawnmower to ascertain for himself whether the mower is safe to operate: such burdens, in the American legal tradition, fall to the supplier of the purchased commodity. What is required is not excluding foreign products from the U.S. stream of commerce that ends with government purchase and use, but rather a set of law-based, economic incentives that require producers to regulate, police, and monitor their own operations to ensure they are selling "pure" (unadulterated, or "espionage-safe" products) to the U.S. government and in U.S. markets. But just as the fact that the manufacturer of the lawn mower has the burden of designing a safe product, the consumer is not relieved of the burden of wearing safety equipment in case of a failure in the manufacturer's design or quality control process that results in a catastrophic failure of the product and potential injury. Prudent counterespionage policy also requires a failsafe process on the U.S. end of the transaction to verify the efforts of the supplying companies, by assessing risk posed by foreign acquisitions of domestic business organizations and by detecting the existence of technically-based espionage devices or apparatus that slip through the company's processes, in order to manage and apportion risk.30

30. One additional method of managing risk, beyond the scope of this writing, is to ensure that no manufacturer has the ability of controlling the destination or end user of particular units of information technology products, and to ensure that a marginal percentage of one company's products are used in applications involving classified, sensitive, or proprietary information. For example, U.S. law might limit U.S. purchases of Lenovo computers to 2% of Lenovo's annual unit product; in the absence of any other controls or factors, this would limit to 2% the likelihood that an adulterated information systems product would be used to process or store sensitive U.S. information or data. Second, the ultimate end-user of any
The issue for analysis, then, is what legal authorities and counterintelligence processes currently exist that can be used, adapted, modified, or amended to counter, through detection and deterrence, technical espionage threats present in goods, such as computers, routers, servers, switches, or mobile phones (host products), manufactured (in whole or in part) or assembled and imported from abroad (both in China and in third countries where Chinese or Chinese-controlled manufacturers are present), used by the U.S. government and the U.S. stream of commerce in the processing and dissemination of classified, sensitive, or U.S.-proprietary information? In more simple terms, how do we use the tools in our kit to stop China from spying on us using our own systems?

I propose a combination of legal processes and information security practices to counter this potential manifestation of a very real threat. Essentially, the modifications and interpretations of law advocated herein shift the onus to the market—manufacturers, assemblers, and distributors—to self-police, to work proactively to control their manufacturing, assembly, and distribution processes to ensure their products are not used in espionage-related activities, while effecting risk-minimization measures. The approach is twofold: prevention through detection and deterrence, and punishment through detection and prosecution:

- Use of the Racketeer Influenced and Corrupt Organizations (RICO) legal regime by the U.S.
Department of Justice to punish, or obtain civil remedies for, espionage by foreign business enterprises, or domestic companies with foreign subsidiaries, and modifying the definition of “espionage” in the racketeering statute to include deliberate or negligent inclusion of, or failure to exclude, espionage-enabling devices, apparatus, or computer code into a product bound for U.S. markets.

- This approach pushes the bounds of anti-criminal enterprise law, prompting Congress to tweak the RICO and espionage statutes to allow the courts to reach business enterprises engaged or involved in espionage, and to force the federal courts to confront RICO’s utility against novel criminally-organized activity, including enterprises designed or recruited to commit espionage, or those which passively, or through willful ignorance, permit their products to be engineered or modified to serve as instruments of espionage.

- RICO criminal penalties can affect the share price of publicly traded companies, and civil remedies can result in seizures of cash and property belonging to the companies engaged in the RICO enterprise – providing a market-based, economic incentive for companies to ensure their products are not modified or altered to enable espionage by foreign powers, or the agents of foreign powers.

- Reforming the Exon-Florio statutory framework underlying the U.S. Department of the Treasury's Committee on Foreign Investments in the United States (CFIUS), incorporating the Intelligence Community Acquisition Risk Center (CARC) into the CFIUS structure, and emplacing new responsibilities on the Defense Technology Security Administration.

- With regard to CFIUS, streamlining the committee’s organization, function, and leadership, with a view toward making it a more effective tool against acquisition of U.S.
business interests by foreign entities that might use the newly-acquired U.S. business to enable espionage by causing or permitting the adulteration of information system manufacturing, assembly and distribution processes.

- Strengthening CFIUS’s investigative resources and remedial powers, particularly with regard to companies, foreign or domestic, potentially engaged in, supporting, or conducting espionage or espionage-related activities.

- Other techniques might include:
  - Prescribing drastic civil remedies, such as divestment or liquidated damages against companies whose products do not pass rigid inspections mandated by statute or Executive Order.
  - Establishment of an aggressive inspection regime of a representative sample of all computers and information system components manufactured, modified, or assembled abroad, designed to detect engineered software and software vulnerabilities designed to provide access for espionage-related purposes.

- Like the RICO economic incentivization, this practice would shift the burden to private companies:
  - To ensure that they engineer counterespionage protections into their manufacturing and shipping processes;
  - To ensure that personnel are properly screened for trustworthiness and loyalty; and
  - To ensure that products are inspected and tested before delivery to U.S. Government customers, because discovery of a national security risk in company’s products could, and should,
lead to decertification by CFIUS and judicial orders to the parent company to divest – an expensive proposition.

Several key assumptions underlie the analysis herein:

1. That China or other foreign powers have the desire to acquire foreign intelligence, both security-related and economic intelligence, from the U.S.

2. That China or other foreign powers have the technological capacity to create or manufacture technical espionage devices, apparatus, or computer code of the type required to capture and transmit information to the receiving foreign entity clandestinely;

3. That China or other foreign powers have the analytical capacity to turn massive volumes of raw data captured from U.S. systems into useful intelligence, beneficial to the foreign power’s security or economy, to the detriment of U.S. security and economy;

4. That devices or code, once inserted into products bound for U.S. consumption and use, generally are difficult, but usually not impossible, to detect;

5. That these devices, apparatus, or code would be detected more easily during the manufacturing, assembly, and/or distribution processes, than after the finished host equipment has entered the U.S. stream of commerce; and,

6. That China or some other foreign power attempting to effect technically-based espionage, could not control or dictate the destination, or end-user, of the adulterated host equipment, and could not ensure that adulterated host equipment is not directed toward certain “target” consumers, such as the CIA, Department of State, Department of Defense, FBI, or certain Congressional committees.

III. RICO AND ESPIONAGE ENTERPRISES

The Racketeering and Corrupt Organizations (RICO) legal regime defines as criminal conduct – and provides civil remedies against RICO-related property related to – organizing, operating,
and profiting from a criminal enterprise. Originally borne from the U.S. campaign against organized crime, specifically established Mafiosi criminal syndicates engaged in traditional criminal activities such as extortion, drug trafficking, protection rackets, usurious and unregulated lending, theft, and gambling, RICO has been found applicable in a wide variety of contexts, including use not only against conventional organized crime, but also against urban drug gangs, mail and wire fraud schemes, and corrupt business practices, and even government civil actions against the tobacco industry.\(^3\) Its utility may not be limited to ordinary criminal enterprises such as new Central American-influenced gang activity\(^3\) that replaced the Italian and Sicilian mafia and Irish mobs that RICO originally was enacted to combat, but might be extended or modify to include terrorism\(^3\) and


RICO was first conceived as a tool to prosecute organized crime, most obviously the Mafia. And its key component lay in assuming the existence of an “enterprise” that crooks manipulated for illegal ends. In the original conception of RICO, this enterprise was a legitimate organization – usually a corporation or labor union – and the crooks committed a RICO violation by laundering criminal profits through or investing them in the enterprise, or by using the otherwise good offices of the enterprise to commit illegal acts. The “act” of racketeering thus simply consists of an individual committing at least two “predicate acts” within 10 years in a manner somehow tied to the enterprise, and those predicate acts can be just about any act constituting a
Technically-Based Espionage Threat

Espionage activities—particularly since RICO's express purpose, essentially, was to criminalize organizing an enterprise to commit criminal offenses.

Terrorist and espionage networks fit the general RICO criminal enterprise category squarely on their faces. For example, where a company permits its manufacturing, assembly or distribution processes to become corrupted by foreign agents, permitting agents to place listening devices or computer code enabling capture, packaging, and transmittal of information or data, the criminal enterprise cognizable under modified-RICO would consist of the company, including its officers, the foreign agent, and the foreign power for whom the agent is acting. Moreover, where two or more actors within the company—particularly actors with "control group" or managerial responsibilities within the company whose actions can be imputed to the company—engage in a pattern of racketeering activity, the company itself might constitute the enterprise. In fact, "courts have found that public entities and governmental agencies, as well as private entities, can constitute RICO enterprises. For example, the term 'enterprise' has been found to encompass private businesses, sole proprietor-ships, corporations, labor organizations, schools, county prosecutors' offices, marriages, and other 'associations in fact.'" 34

A. History of the RICO Statute

The RICO statute 35 was passed in 1970 with the specific aim of providing a federal statutory framework for attacking organized crime under state or federal law. ... Moreover, the enterprise need not have a pecuniary goal—a shared ideology is fine, so long as the racketeering activity meets the trivially easy test of affecting interstate commerce. The government can now map the concept of an enterprise onto almost any kind of criminal organization, call it a RICO enterprise, then prosecute anyone working for that enterprise of a RICO violation. ...

[C]alling al-Qaeda a RICO enterprise would add color to an already dramatic case and it might just help the government sprinkle the magical federal conspiracy dust on an even wider group of characters. Congress has supplied a special instrument to combat large, conspiratorial organizations; the government should try to sell it to jurors.

crime organizations. The statute's "secret weapons" are civil proceedings against property acquired in connection with the enterprise, and enhanced criminal punishment – for simply organizing into a criminal business unit to accomplishing criminal enterprise, or "racketeering activity," some of which, by statutory definition, frequently consists of traditional state crimes, on the theory that such a business organization injures interstate commerce. The statute's preliminary 'Statement of Finding and Purpose' declares that "[i]t is the purpose of [RICO] to seek the eradication of organized crime in the United States by strengthening the legal tools in the evidence-gathering process, by establishing new penal prohibitions, and by providing enhanced sanctions and new remedies to deal with the unlawful activities of those engaged in organized crime,"36 a purpose that Congress may embrace through minor modification of the statute to redefine espionage and encompass organized espionage enterprises.

The RICO statute defines "racketeering activity" as state law felonies such as murder, kidnapping, arson, gambling, robbery, bribery, extortion, obscenity, and controlled substances, as well as a wide variety of specific federal offenses, such as mail fraud, wire fraud, obstruction of justice, witness tampering, trafficking in various contraband, and other frauds relating generally to interstate commerce.37 It essentially prohibits maintenance of an ownership or management interest in an enterprise engaged in racketeering activity; profiting from or participating in the activities from such an enterprise; and conspiring to violate these prohibitions – in other words, however "racketeering activity" is defined (a term which definition has been regularly expanded by Congress), RICO "merely imposes additional liability on those who commit certain offenses repeatedly."38 The statute, as worded, does not plainly touch espionage-related activities, except, possibly, on a fact-dependent basis:

1. Through a hyper-aggressive reading of the federal

wire fraud statute as a component of RICO-prohibited activity;\(^3\)
2. Possibly in connection with mail fraud\(^4\) (if the mail is used in connection with the espionage activity); or
3. By invoking the access devices fraud provision.\(^4\)

Each of these prohibitions only arguably would reach espionage activities, and probably only in certain circumstances. A much safer bet to ensure the law's reach would be to engraft an espionage component into the definition of "racketeering."

---

39. The federal wire fraud statute, 18 U.S.C. §1343 (Supp. IV 2004), states:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

The government would have to stretch the definition to a near-implausible degree, that wire fraud is constituted by modifying computers as instruments of espionage which are then sold or delivered to the U.S. government, making the U.S. government the wire fraud victim. In such a reading, the fraudulent activity element is that the government paid full value for and received a product designed or engineered to act contrary to its interests, or, in any case, a product not identical to the goods intended to be purchased. This argument assumes that wire transmissions were utilized at some point during the transaction, such as email messages to coordinate the sale, telephone calls, electronic transmission of payment documents, etc.

40. See 18 U.S.C. § 1341 (Supp. IV. 2004). Like the wire fraud provision, invoking this provision to reach espionage, however, would require framing the espionage activity as somehow defrauding the targeted recipient of the goods.

41. 18 U.S.C. §1029 (2000). This provision prohibits fraud against telecommunications service providers by modifying devices or software. It is probably inapplicable to technically-based espionage activity, as the intent of the statute is to prevent fraud, or, essentially, theft of services, not theft of protected information.
B. Fine-tuning and Utilizing RICO to Achieve Counterespionage Benefits

1. Criminal Enterprise Liability

With minor modification – by inserting “espionage activities”42 into § 1961(1) of the RICO statute, and defining this term elsewhere in the statute, such as by inserting a definition at §1961(11) – prosecutors could rely on Congress’ instructions to the courts to interpret RICO liberally43 to reach espionage enterprises, including corporations who allow their products, through design or by neglect, to become corrupted with espionage instruments – particularly those corporations whose components are manufactured or assembled overseas. “Espionage activity” could be defined as “an act, communication, or failure to act to prevent an act or communication, the purpose of which is to effect the compromise of classified information [as defined in classified information protection statutes], government proprietary information, or commercial proprietary information [as defined in the Economic Espionage Act], to a foreign power or agents of a foreign power, including foreign states, organizations, or non-state actors or enterprises, with the intent or foreseeable effect of injuring national security.” This wording, or some version of it, would bring within RICO’s reach deliberate acts of espionage, and failures by companies supplying goods to the U.S. stream of commerce and domestic customers, including the federal government to protect their products from technically-based espionage-enabling adulteration. Legislative drafters can wordsmith the statute through a detailed analysis of leading products liability standards, extracting the strict liability concepts and applying them to the espionage statute, in order to impose, at law, an affirmative duty on companies to control their business processes to avoid the introduction of technical espionage devices, apparatus, or code.44 The intent is to lower the degree of

42. This term should be defined in the statute with reference to Chapters 37 (Espionage and Censorship) and 90 (Protection of Trade Secrets) of Title 18, U.S. Code.


44. An exhaustive analysis of products liability legal standards and adjustment of these articulated standards to apply to espionage activities is
culpability required to be shown of companies introducing adulterated information technology products into the U.S. stream of commerce, in order to make them, essentially, involuntary partners in the counterespionage enterprise, by requiring them to monitor their manufacturing, assembly and distribution processes with sufficient care to avoid application of the statute.

The statute is hardly legislatively untouchable: historically, Congress has not been reluctant to modify RICO to bring more activities within its reach: commentators Sacks, Coale, and Goldberg note that

---

beyond the scope of this paper. For a primer on general products liability, see Products Liability, http://www.law.cornell.edu/wex/index.php/Products_liability (last visited May 10, 2006) ("Products liability refers to the liability of any or all parties along the chain of manufacture of any product for damage caused by that product. This includes the manufacturer of component parts (at the top of the chain), an assembling manufacturer, the wholesaler, and the retail store owner (at the bottom of the chain). Products containing inherent defects that cause harm to a consumer of the product, or someone to whom the product was loaned, given, etc., are the subjects of products liability suits. While products are generally thought of as tangible personal property, products liability has stretched that definition to include intangibles (gas), naturals (pets), real estate (house), and writings (navigational charts).

"Products liability claims can be based on negligence, strict liability, or breach of warranty of fitness depending on the jurisdiction within which the claim is based. Many states have enacted comprehensive products liability statutes. These statutory provisions can be very diverse such that the United States Department of Commerce has promulgated a Model Uniform Products Liability Act (MUPLA) for voluntary use by the states. There is no federal products liability law.

"In any jurisdiction one must prove that the product is defective. There are three types of product defects that incur liability in manufacturers and suppliers: design defects, manufacturing defects, and defects in marketing. Design defects are inherent; they exist before the product is manufactured. While the item might serve its purpose well, it can be unreasonably dangerous to use due to a design flaw. On the other hand, manufacturing defects occur during the construction or production of the item. Only a few out of many products of the same type are flawed in this case. Defects in marketing deal with improper instructions and failures to warn consumers of latent dangers in the product.

"Products Liability is generally considered a strict liability offense. Strict liability wrongs do not depend on the degree of carefulness by the defendant. Translated to products liability terms, a defendant is liable when it is shown that the product is defective. It is irrelevant whether the manufacturer or supplier exercised great care; if there is a defect in the product that causes harm, he or she will be liable for it.") (emphasis added).
In the Comprehensive Crime Control Act of 1984, Congress extended the definition of "racketeering activities" under RICO to include dealing in obscene materials, as well as the non-reporting of currency and foreign transactions. The Antiterrorism and Effective Death Penalty Act of 1996 further extended the RICO provisions to include various immigration crimes.  

Other amendments since the statute's original enactment include adding to the definition of racketeering activity trafficking in stolen cigarettes, motor vehicles, and automotive parts, murder-for-hire, sexual exploitation of children, money laundering, witness tampering or retaliation, obstruction of justice, and bankruptcy fraud. The political momentum backing security concerns at present might be leveraged to convince Congress to make such minor amendments to the statute to bring espionage, by state-based agents or terrorists, within the reach of the potent RICO provisions. Such a modification would effect an enhancement of security at a very small price in civil liberties, in that there is no civil right or liberty to be free from a RICO prosecution where evidence shows complicity, deliberate or otherwise, in espionage or espionage-related activities; moreover, business organizations, as artificial legal constructs, do not traditionally enjoy the same degree of fundamental civil liberties as those exercised by natural persons. Burdening of a company in the manner contemplated comes with no "liberty" price tag attached, only a financial cost for the company to monitor more closely its business operations.

2. Civil RICO Enforcement

Moreover, the statute provides a complimentary civil component, which could be exercised in favor of the United States, to "attack the economic roots of racketeering activities." Not only is the Attorney General granted specific authority to bring actions in equity to enjoin or judicially limit the operation of an unlawful RICO enterprise and order civil forfeitures, requiring
disgorgement of all proceeds of the enterprise.\textsuperscript{48} the U.S. Government itself may pursue legal, compensatory remedies against the enterprise, where the government is the damaged party.\textsuperscript{49} Section 1964(c) of the RICO statute permits any "person" injured to sue in federal court to recover treble damages based on economic injury sustained, plus attorney's fees and litigation expenses.\textsuperscript{50} "Person" is defined in the statute as "any individual or entity capable of holding a legal or beneficial interest in property."\textsuperscript{51} The government is clearly an "entity" within a plain language meaning of that word — "a thing with distinct and independent existence"\textsuperscript{52} — and the government certainly holds legal title to billions of dollars worth of real property, goods, and chattels.

Where the government could show an injury to its pecuniary interest or property, an amended "espionage RICO" does not preclude the government from recovering money from the corporation, even a foreign corporation, supplying the espionage-engineered systems.\textsuperscript{53} Either theory of recovery of ill-gotten RICO proceeds through civil forfeitures would work as a powerful incentive to business organizations to "espionage-proof" their

\begin{itemize}
  \item \textsuperscript{48} 18 U.S.C. §1964(a) (2000)("The district courts of the United States shall have jurisdiction to prevent and restrain violations of section 1962 of this chapter by issuing appropriate orders, including, but not limited to: ordering any person to divest himself of any interest, direct or indirect, in any enterprise; imposing reasonable restrictions on the future activities or investments of any person, including, but not limited to, prohibiting any person from engaging in the same type of endeavor as the enterprise engaged in, the activities of which affect interstate or foreign commerce; or ordering dissolution or reorganization of any enterprise, making due provision for the rights of innocent persons."); \textit{see also} Marian R. Williams, 27 CRIM. JUST. REV. 321, 322-23 (2002) (noting that government entities retain 100% of all assets forfeited through civil actions).
  \item \textsuperscript{49} \textit{See} 18 U.S.C. §1964(c).
  \item \textsuperscript{50} \textit{Id.}
  \item \textsuperscript{51} 18 U.S.C. §1961(3).
  \item \textsuperscript{52} COMPACT OXFORD ENGLISH DICTIONARY, http://www.askoxford.com/concise_oed/entity?view=uk (last visited April 29, 2006).
\end{itemize}
manufacturing and distribution processes, shifting the burden to companies to ensure their products are not modified by employees or agents of foreign governments or non-state actors, such as foreign organized crime syndicates or transnational terrorists.

3. Application and Benefits of Reaching Espionage Activities Through RICO

In addition to extending personal criminal prosecutions and civil liability to culpable company executives proven to have been complicit in the decision to modify information technology products as instruments of espionage, RICO is capable, with minor modification, of reaching the business organization itself, such as the computer manufacturing corporation Lenovo, or other similarly situated corporations, companies or partnerships. Again, "person" is defined in the statute as "any individual or entity capable of holding a legal or beneficial interest in property," and "enterprise" includes "any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity." This broad definition of "person" sweeps in natural persons, trusts, and various forms of business organization, including partnerships and corporations – which meet the dual criteria of "legal entity" and "capable of owning property."

The statutory definition of "enterprise," however, also would need minor tweaking, as the term "any union or group of individuals associated in fact" would probably require modification to "any union or group of individuals and/or entities associated in fact." This would enable RICO to reach a corporation or other legal "person" by virtue of participating in the espionage "association in fact" enterprise, but only where the definition of enterprise is expanded to include a foreign government – an entity – as "partner" to the corporation’s legal personality. Neither the foreign government nor the business organization is an

56. Reply Brief of Petitioner at 1, Mohawk Indus., Inc. v. Williams, 126 S. Ct. 2016 (2006) (No. 05-465) ("RICO is aimed at the misuse of a distinct 'enterprise.' Indeed, the statutory limitations make plain that only individuals – not an ad-hoc grouping of a corporation and others – can form an association-in-fact enterprise.")
“individual” under any reading of the statute. Because the foreign government is not an “individual” but could be considered an “entity,” the definition of “enterprise” should be adjusted to reach the foreign government for the purpose of bringing the business organization (not the foreign government) into RICO’s jurisdictional reach.⁵⁷ Criminal proceedings against a company-defendant can cripple the company’s economic worth and essentially drive it out of business by making the company’s shares valueless,⁵⁸ another robust enticement for companies to ensure their products are not involved in the business of spying. In sum, by forcing the companies to self-police their products against espionage-related corruption in the manufacturing, assembly, and distribution processes, U.S. counterintelligence efforts can be augmented by companies seeking to do business with the U.S. government or, in the case of economic espionage, with U.S. business organizations.

Assuming Congress acts to bring espionage activities within the definition of “racketeering,”⁵⁹ RICO permits the introduction of a broad range of evidence to prove up the racketeering conspiracy – transactions that would be not relevant to proving a predicate criminal offense within the range of offenses included in

---

⁵⁷. The concept of expanding the jurisdiction of RICO through interpretation of the definitions is not without controversy. See Toni Locy, Court is Asked to Expand Racketeering Law’s Reach, BOSTON GLOBE, Apr. 27, 2006, available at http://www.boston.com/news/nation/washington/articles/2006/04/27/court_is_ asked_to_expand_ racketeering_laws_reach (noting comments by Justices during oral argument supportive of the petitioner’s position and probing the wisdom of expanding the definition of “enterprise” in the RICO statute beyond what Congress clearly intended to proscribe.).


⁵⁹. “Racketeering” is an elastic concept that has an ordinary usage relating to organized crime but which, like any term in a statute, is susceptible to modification by a clearly expressed intention of Congress. Much academic and judicial criticism has been made of government attempts to shoehorn more and more conduct into the existing definition of racketeering; in order to avoid such criticism, Congress should act to redefine the term to remove ambiguity regarding whether racketeering includes espionage-related activity.
the definition of "racketeering," could be used to paint the broader picture of the enterprise. By charging espionage-enabling engineering modifications in products sold to the U.S. as RICO espionage racketeering, the government could bring to the light of day the actions of a whole litany of actors whose actions might otherwise not be provable in an ordinary criminal trial, such as the acts of minor unindicted co-conspiratorial participants in the enterprise whose conduct might be ruled not legally relevant to establishing the principal espionage case. Finally, RICO counts in an indictment would enable the government to add twenty years of confinement punishment to the sentence upon conviction for espionage and RICO violations, subject to U.S. Sentencing Guidelines calculus.\textsuperscript{60} Wielding RICO as a counterespionage tool would enable the government to provide a more powerful disincentive for companies to permit their employees or facilities to be involved in technically-based espionage activities.

Finally, a corollary procedure would be useful to preventing foreign influence over U.S. business organizations whose manufacturing, assembly and distribution processes represent opportunities for foreign powers to collect information in the first place. Such a procedure could be effected by modifying the legislative authority for the existence and functioning of the Committee on Foreign Investment in the United States (CFIUS).

IV. STRENGTHENING CFIUS AND CARC BY REFORMING EXON-FLORIO

A. CFIUS Background and the Dubai World Ports Controversy

Foreign direct investment (FDI) in U.S. markets has historically been met with open arms. Foreign investment in U.S. corporations or business organizations, however, has the potential to compromise the companies to the detriment of U.S. national security. With this in mind, Congress acted in Section 5021 of the Omnibus Trade and Competitiveness Act of 1988, amending the Section 721 of the Defense Production Act of 1950,\textsuperscript{61} to provide a review mechanism to the president, granting him the power to forbid or mandate alterations to any purchase, merger, takeover,

\textsuperscript{60} See generally\ United States Sentencing Guidelines Manual (2005).
2007] TECHNICALLY-BASED ESPIONAGE THREAT 857

or controlling investment in a U.S. company when the transaction is shown to be detrimental to U.S. national security. The Exon-Florio statute empowered the president to establish CFIUS. CFIUS most recently received extended press coverage over its approval of the Dubai Ports World (Dubai World) port operations deal, in which Dubai World sought to purchase the U.K. company Peninsular and Oriental Steam Navigation Company, which held major port terminal operations contracts in the U.S. The transaction would have given UAE government-owned Dubai World "control of substantial operating functions at a number of major East and Gulf Coast Ports, including New York, Newark, Philadelphia, Baltimore, Miami, and New Orleans...[and would acquire lesser, yet important, operating functions] at ports including Portland [Maine], Boston, Davisville [Rhode Island], Norfolk, Galveston, Houston, and Corpus Christi." The Dubai World transaction created a political hullabaloo. CFIUS detractor Senator Paul Sarbanes' pointed out that the committee's decision not even to refer the transaction for a detailed, 45-day investigation constituted an egregious failure of the body to function as designed, an oversight reminiscent of a similar controversy in 2005, in which the Chinese government-controlled China National Offshore Oil Corporation (CNOOC) attempted to acquire U.S. energy company Unocal. For some, the threat to U.S. port security represented by the Dubai World proposed transaction—which has attained a special level of

62. 50 U.S.C.App. § 2170(c) (1988)
sensitivity with regard to the role of port security in preventing
the introduction of a terrorist nuclear device inside U.S. borders — posed by this transaction was obvious, simply from the ethnic
(Arab) identify of one of the parties to the transaction. This is a fairly clear case of ethnic profiling, against a company and a
government, rather than an individual or group of individuals,
that may or may not be supported by evidence regarding United
Arab Emirates (U.A.E.) government support to terrorism, and
may or may not be justified or justifiable. But for almost
everyone, scrutiny of the functioning of CFIUS in the Dubai World
affair would be an important and valuable test case as to whether
CFIUS was functioning as designed, and as to whether the design
should be revised.

The Dubai port transaction press scrutiny highlighted confusion in the general public, and provoked furor and

---


68. But see Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission Report), Monograph on Terrorist Financing, Staff Report to the Commission 6, (2004), available at http://www.9-11commission.gov/staff_statements/911_TerrFin_Ch1.pdf (last visited May 3, 2006) (“The U.S. government had recognized the value of enlisting the international community in efforts to stop the flow of money to al Qaeda entities. U.S. diplomatic efforts had succeeded in persuading the United Nations to sanction Bin Ladin economically, but such sanctions were largely ineffective. Saudi Arabia and the U.A.E., necessary partners in any realistic effort to stem the financing of terror, were ambivalent and selectively cooperative in assisting the United States.”). Political opposition to U.A.E. investments in the U.S. may very well be an orchestrated governmental signal to partners in the global war on terror that it really is the world’s largest economy that holds most of the cards — economic revenge for U.A.E. foot-dragging on counterterrorism collaboration designed to intimidate the wisdom of cooperating with the U.S. strategic agenda.

69. One well-respected commentator posits that the possibility of that strict scrutiny of equal protection challenges may yield permissible race-based distinctions in wartime, because the depth and breadth of the government’s compelling need for security increases exponentially. See Mark Tushnet, Emergencies and the Idea of Constitutionalism, in The Constitution in Wartime: Beyond Alarmism and Complacency 39, 39 (Mark Tushnet ed., 2005) (“A race-based classification that would be unconstitutional during peacetime might be constitutional during wartime, not because the constitutional standards differ, but because their rational application leads to different results.”).
grandstanding in Congress,\textsuperscript{70} over how business transactions dealing with "suspect states" (concern emerged over the fact that the company, obviously based in Dubai, U.A.E. – an Arab state known to produce terrorists\textsuperscript{71} and suspected of complicity by some

\textsuperscript{70} H.J. Res. 79, 109th Cong. (2006) (Joint Resolution disapproving the results of the review conducted by the Committee on Foreign Investment in the United States (CFIUS) into the purchase of Peninsular and Oriental Steam Navigation (P&O) by Dubai Ports World (DP World); S.J. Res. 32, 109th Cong. (2d Sess. 2006) (Joint Resolution disapproving the results of the review conducted by the Committee on Foreign Investment in the United States (CFIUS) into the purchase of Peninsular and Oriental Steam Navigation (P&O) by Dubai Ports World).

\textsuperscript{71} As opposed, perhaps, to the U.S. and the U.K., both non-Arab states known to produce terrorists. While the U.A.E.'s official position is one of resolute support for the U.S. campaign against terrorism, see U.A.E. Foreign Policy, \url{http://uae-embassy.org/htmlpages/ForeignPolicy.htm} ("In common with the rest of the world, the United Arab Emirates found in the latter part of 2001 that a major part of its foreign policy concerns was the international campaign against terrorism that developed after the 11 September attacks against Washington and New York. The U.A.E.'s condemnation of the attacks, in which over 4000 people died, was swift and total.

"At this time of tragedy, our hearts are filled with sadness and compassion for the victims of the terrible and criminal acts that took place in New York and Washington ... and we send again our condolences to you, the people of the United States and, in particular, the families of the victims,' Sheikh Zayed told President Bush in a message shortly after the attacks.

"We have noted your wise, resolute and timely remarks about the necessity for these tragic events not to be used as an excuse for, or reason for, any attacks against or hostility towards Arab Americans or Americans of the Muslim faith ... We share with you the belief that the acts ... are utterly repugnant in the eyes of Islam, and we thank you for your timely and appropriate statement, which so well reflects the values and traditions of the United States as a land where neither racial origin nor religious beliefs is a disqualification from full membership of the American nation. ..."

"[On] the occasion of the country's thirtieth National Day, Sheikh Zayed added that: terrorism is the enemy of all humanity ... We support international legitimacy in every action and measure that it takes to combat terrorism and eradicate it and to close the way for terrorists ... Terrorism is an international phenomenon that has no religion or race.

"The readiness of the United Arab Emirates to collaborate with the international campaign against terrorism was quickly displayed....), the government has been accused by some commentators of turning a blind eye to terror financing through the U.A.E. ... See id. ("In recognition of the fact that the fight against terrorism required not only a military response, but also a concerted effort to identify and eradicate its network of financial and other links, the U.A.E. authorities responded rapidly to requests from the United States to identify and freeze any bank accounts used by suspect individuals and organizations. Although some evidence of suspect money transfers through, rather than to, the U.A.E. were identified, an intensive review by
in terrorist financing) are scrutinized by the U.S. government—this, despite the absence of public domain information suggesting that the transaction represented a national security liability. For its part, the Bush administration seemed to be caught flatfooted by the fact that the transaction had been approved, in fact, by two organizations in his administration, and exercised executive power to rescind the recommended approval by CFIUS and force further scrutiny of the transaction.\textsuperscript{72} The response of the government and the press to the transaction was an obvious political defensive reaction, which resulted in Dubai World’s withdrawal of their offer for the acquisition.\textsuperscript{73} This was due to a

\textsuperscript{72} See Political Backlash Over Port Deal, CBS News, Feb. 22, 2006, http://www.cbsnews.com/stories/2006/02/22/national/main1335774.shtml (last visited May 10, 2006) (“If there is one thing Congressional leaders and the White House can agree on, it is that neither knew the port deal with a United Arab Emirates company was even in the works ... President Bush was unaware of the pending sale of shipping operations at six major U.S. seaports to a state-owned business in the United Arab Emirates until the deal already had been approved by his administration ... Defending the deal anew, the administration also said that it should have briefed Congress sooner about the transaction, which has triggered a major political backlash among both Republicans and Democrats.”)

\textsuperscript{73} Jacob Freedman, Initial Hill Reaction Muted to New Dubai Acquisition, CONG. Q., Apr. 28, 2006. (“The White House announced [today] that President Bush has approved another sensitive U.S. acquisition by a Dubai-owned company, but its careful handling of the review appears to have averted the kind of public and congressional backlash that sank the DP World ports transaction. The acquisition of British Doncasters Group Ltd. by Dubai International Capital was subject to a full 45-day investigation by the Committee on Foreign Investment in the United States (CFIUS). The administration notified several congressional committees when it began the investigation and briefed them on its details. In contrast, approval of DP World’s acquisition of a British terminal operator with port operations in the United States occurred without a detailed, 45-day security investigation. Congress and senior administration officials [including the President] were unaware of the deal until it was reported by the news media. After a public uproar, DP World agreed to sell off its U.S. operations in the face of fierce congressional opposition. Doncasters has several manufacturing plants in the Georgia, Connecticut and other states that make precision parts for aerospace and other industrial uses, both civilian and military ... as part of the deal’s approval, Dubai International Capital signed a binding agreement that it would maintain uninterrupted supplies to the Department of Defense....” There are two differences between this deal and the Dubai Ports deal. First, this went through the process in a careful, thoughtful way; and second, this is a product, not a service, and the opportunity to infiltrate and
perception, accurate or erroneous, that CFIUS review was conducted inadequately, which may reflect a lack of press and Congressional understanding of the process. Or it may have simply been an expedient political sitting duck, which allowed political critics to score domestic “homeland security” points with constituents, at substantial political cost to the Bush administration and very little fiscal cost in FDI — the money changed hands between the U.K. and the U.A.E. entities only.

Since the Dubai World fiasco, CFIUS has approved, and the President has permitted to go forward, another sensitive acquisition by a Dubai company, a subsidiary of Dubai Holding LLC, of Ross Catherall US Holdings Inc. (Ross Catherall), a U.S. subsidiary of British Doncasters Group that manufacturers turbine fan parts and airfoils for military tanks and helicopters — this time after a full, 45-day investigation and proper review. Nevertheless, Congress has vowed to overhaul the CFIUS system because of perceptions of defects in its design and operation. Ensuring CFIUS functions effectively through legislative reform will reap national security benefits generally by ensuring a careful screening of foreign holdings of U.S. business enterprises. Specifically, with regard to the Chinese technology-based espionage threat, CFIUS review can mitigate or eliminate foreign acquisition of U.S. business interests that would pave the way for the introduction of espionage-enabling devices, apparatus, or code into information technology host equipment destined for U.S.

sabotage is both more difficult and more detectable,’ [Senator Charles] Schumer said. Congressional leaders have said that the CFIUS process needs to be made more transparent, with a greater role for Congress. The Senate Banking, Housing and Urban Affairs committee approved a measure on March 30 that would overhaul the foreign investment review process. On the House side, Majority Whip Roy Blunt ... said Thursday that he will introduce a bill by Memorial Day. Richard C. Shelby ... chairman of the Senate committee, said in a statement Friday that he was ‘encouraged to see that the appropriate process was followed by CFIUS’ in the Doncaster transaction. But he said he remains ‘committed to continue to press for an overhaul of CFIUS to bring accountability, transparency and confidence to the process.”)

76. See Freedman, supra note 73; Sarbanes statement, supra note 65.
consumption.

B. CFIUS Design, Legal Standards, and Operation

CFIUS is an interagency group chaired by the Department of the Treasury, with the head of Treasury's Office of International Investment serving as the Staff Chair,\(^7\) making CFIUS a largely Treasury-centric show by virtue of the Department’s capture of the CFIUS leadership group. CFIUS enjoys representation from the Departments of State, Defense, Justice, Commerce, and Homeland Security, as well as the Office of Management and Budget, Chairman of the Council of Economic Advisors, U.S. Trade Representative, the Director of the Office of Science and Technology Policy, the National Security Council, and the Assistant to the President for Economic Policy, and, occasionally, depending on the nature of the transaction being reviewed, the Departments of Energy and Transportation and the Nuclear Regulatory Commission.\(^7\) CFIUS is tasked with the mandate to review the foreign acquisition of U.S. businesses or business interests for national security impacts or concerns.\(^7\)

Exon-Florio provides certain standards against which CFIUS review must be conducted in order to inform and enable the President to act to suspend or prohibit foreign acquisition of a U.S. company:

- Whether "[t]here is credible evidence that leads [the President] to believe that the foreign investor might take action that threatens to impair the national security";\(^8\) and
- Whether "[e]xisting laws, other than the International Emergency Economic Powers Act (IEEPA) and the Exon-Florio amendment itself, do not in his judgment provide adequate and appropriate authority to protect

\(^7\) See Testimony Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, Mar. 2, 2006 (testimony of Robert M. Kimmitt, Deputy Secretary, U.S. Department of the Treasury) [hereinafter Kimmitt testimony]; Testimony Before the U.S. House of Representatives Committee on Armed Services, Mar. 2, 2006 (testimony of Clay Lowery, Assistant Secretary (International Affairs), U.S. Department of the Treasury).

\(^8\) See Kimmitt testimony, supra note 77.
the national security."\textsuperscript{81}

The FY 1993 National Defense Authorization Act for Fiscal Year 1993 amended Exon-Florio, requiring an investigation where "the acquirer is controlled by or acting on behalf of a foreign government and the acquisition "could result in control of a person engaged in interstate commerce in the U.S. that could affect the national security of the U.S."\textsuperscript{82} This provision enabled CFIUS to examine the proposed Dubai World transaction, which was essentially an acquisition of a U.K. company by a UAE entity. The U.S. connection was that the U.K. company, which employed U.S. workers whose duty performance in port operations could affect national security, was being acquired by another foreign entity.

In conducting the national security review, the five factors for consideration are:

1. domestic production needed for projected national defense requirements;
2. the capability and capacity of domestic industries to meet national defense requirements . . . ;
3. the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the U.S. to meet the requirements of national security;
4. the potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to a country that supports terrorism or proliferates missile technology or chemical, [nuclear], and biological weapons; and
5. the potential effects of the proposed or pending transaction on U.S. international technological

\textsuperscript{81} 50 U.S.C. §§ 1701-1706 (1977). The statute delegates authority to the President to take extraordinary measures during wartime or times of national emergency to deal with "unusual and extraordinary" threats. The measures include prohibiting or restricting certain foreign commercial transactions, currency exchanges, foreign investment, and certain exports and imports. \textit{Id. at} § 1701.

leadership in areas affecting U.S. national security.\textsuperscript{83} An additional, unstated factor is frequently considered, which in reality is a procedural factor which affects the other five: what remedial or confidence-building measures can the parties to the review undertake to limit the actual or perceived threat to national security.

Most, if not all, of these factors were clearly implicated by the Dubai World deal, and by the Lenovo acquisition of IBM's PC division. The question, then, becomes whether the effects may be remedied by other provisions of law, or whether other prophylactic mechanisms can eliminate or reduce the vulnerability. Where review indicates potential vulnerabilities, CFIUS and its constituent members work with the acquiring and acquired companies to ensure the emplacement of certain safeguards to remedy the concern. For example, the government can mandate, as a precursor to approval,

Special Security Agreements, which provide security protection for classified or other sensitive contracts; Board Resolutions, which, for instance, require a U.S. company to certify that the foreign investor will not have access to particular information or influence over particular contracts; Proxy Agreements, which isolate the foreign acquirer from any control or influence over the U.S. company, and Network Security Agreements (NSAs).\textsuperscript{84}

During the CFIUS 30-day review period of the Dubai World transaction, CFIUS member Department of Homeland Security negotiated an “assurances letter” with the Dubai World and the acquired company, P&O,\textsuperscript{85} in which, presumably, the company agreed not to sponsor terrorist attacks inside the U.S.

The Exon-Florio/CFIUS process represents a check on foreign governments or entities gaining control over U.S. business organizations to the detriment of U.S. national security. With

\textsuperscript{83} See id.
\textsuperscript{84} See Kimmitt testimony, supra note 77.
some minor modifications by Congress, however, CFIUS, or a new subsidiary or peer organization, could become an even more effective guarantor of security in its review of business transactions, particularly purchases of computer/information technology equipment to be used in U.S. government offices exercising national security/foreign affairs functions, such as the intelligence agencies, Departments of Defense, State, Transportation and Homeland Security, FBI, certain sections of the Department of Justice, Congress, and segments of the U.S. courts cleared to hear classified information (e.g., FISA courts). Specifically, CFIUS, or a similar or subsidiary organization, could be empowered by Congress to investigate and certify, through reverse engineering or technical exploitation of a representative sampling of U.S. government-purchased computer/IT products of:

- Foreign companies;
- U.S. companies engaging in manufacturing and assembly of products or components overseas;
- U.S. companies engaging in manufacturing and assembly of products from components manufactured or assembled overseas; and
- U.S. companies purchased or controlled by foreign business organizations or entities.

C. Recommendations for Exon-Florio Reform

Concerns with the efficient functioning of the Exon-Florio/CFIUS process are not limited to those raised by this author. In fact, in 2004, Senators Shelby, Bayh, and Sarbanes wrote to the Government Accountability Office (GAO) (formerly known as the General Accounting Office) requesting a report on the functioning of the CFIUS process.\(^86\) GAO’s 2005 report\(^87\) identified several points of concern, including that the Department of Treasury “narrowly defines what constitutes ‘national security’; that CFIUS is reluctant to start 45 day formal investigations because they perceive a negative impact on foreign investment and a conflict with U.S. open investment policy; that

\(^{86}\) See Lee & Perkins, supra note 66.

the resulting limitation of the CFIUS process to a 30-day preliminary review period makes careful analysis very difficult at best; and that failure to proceed to an investigation means that few Presidential decisions will ever be required, thereby eliminating reporting to the Congress and making Congressional oversight impossible."

The GAO report noted that the narrow definition of "national security," which was formalistic and did not consider, for example, economic and energy security as components of national security, would benefit from CFIUS interpretive expansion of the term's meaning. Moreover, GAO found that the reluctance to initiate a formal (45-day) investigation was, in part, a desire to facilitate FDI, for fear that reading the investigation requirement too broadly would discourage companies from trying to start businesses in the U.S. The GAO report sensibly recommended amendment of Exon-Florio to be more clear regarding the facts that influence whether an investigation should commence; to provide reallocated time to the truncated timeline to permit thorough investigation and decisionmaking; tracking of applications for CFIUS subsequently withdrawn in order to fix highlighted problems that could not be fixed within the mandated timetable that are never re-filed (in other words, ensuring that companies that withdraw from the approval process are courted and convinced to resubmit, to ensure that investment opportunities do not disappear for lack of follow-up, or to ensure that transactions do not proceed sub-rosa and unapproved); and more robust reporting requirements to Congress.

As of March 2, 2006, CFIUS had reviewed 1,604 foreign acquisitions of U.S. companies or business interests, with its last mandatory report to Congress regarding presidential action on CFIUS investigatory recommendations occurring with regard to a transaction between Singapore Technologies Telemedia and Global Crossing, in September 2003. Absent more detailed, year-by-year statistics not readily available, 1600 reviews over 18 years averages about 89 reviews each year. As of December, 2005,  

88. See Sarbanes statement, supra note 65.
89. See GAO Report, supra note 87 at 11.
90. See id at 11.
91. See id at 39-46.; see also Lee & Perkins, supra note 66.
92. See Kimmitt testimony, supra note 77.
CFIUS had initiated 45-day formal investigations (as opposed to the initial 30-day review) in only 25 cases out of about 1600 reviews.\(^9\) Of these 25 investigations, only 12 post-investigation cases were presented to the president,\(^9\) resulting in a single presidential decision to disapprove a transaction and order divestment, in the 1990 attempt by the Chinese-government owned China National Aero-Technology Import and Export Corporation (CATIC) to take over MAMCO Inc., a U.S. manufacturer of metal civilian aircraft components.\(^5\) The last mandatory report to Congress following presidential action on an investigation (a transaction approval) occurred almost three years ago.\(^6\) The reason for the dearth of CFIUS "45-day" investigations and presidential actions is ambiguous. Absent more information regarding the quality of CFIUS review, it is apparent that CFIUS's review process does not frequently result in investigation or presidential decision, much less denial. This may be a result of companies' willingness to effect remedial measures – which may be token measures or may be effective resolutions – to address potential problems or concerns during the pre-filing informal consultative stages, as much as it may be a result of an insufficiently exacting review process. The quality and quantity of CFIUS review is worth continued empirical, detailed analysis by Congress' investigative arm, the GAO, particularly in light of CFIUS approval of the politically-hot (and facially suspect) Dubai ports and Lenovo-IBM deals.

I concur with the GAO recommendations, and add recommendations regarding the 30/45/15 day timeline: that Congress should request an additional GAO follow-up report, and or draft remedial legislation,\(^9\) on several precise issues:

\(^9\) Three bills have already been introduced to reform CFIUS: H.R. 4917, 109th Cong. (2d Sess. 2006), To amend the Defense Production Act of 1950 to require notification to Congress after receipt of written notification of proposed or pending mergers, acquisitions, or takeovers subject to investigation under such Act, and for other purposes; S. 2442, 109th Cong. (2d Sess. 2006), To require the President or the Committee on Foreign Investment in the United States to submit to Congress draft investigation reports on national security related investigations, to address mandatory
1. Consider whether a remedial measure, such as an assurances letter, or a Special Security Agreement or Board Resolution by IBM or Lenovo, would prevent Chinese introduction of "spyware" into computers engineered to gather and transmit data to Chinese government client servers. How does the U.S. Government wield a Board Resolution to stop a determined, clandestine spy inserting technical listening or transmitting devices into computers manufactured for use by U.S. government agencies, or companies that will store valuable proprietary information on the computers – particularly where the board is under the thumb of the rival state government? The Board Resolution is an inadequate remedy: if a company or agent of the company is found to be violating the Board Resolution, civil remedies may arise, including divestment. But in the meantime, the damage is done – the horse, in the form of U.S. classified or proprietary information, will have left the barn of information security. What is required are more exacting standards of review – including initial and continuous physical inspections of equipment produced and sold by CFIUS-reviewed business enterprises, and of equipment produced and sold to the U.S. government and U.S. companies for domestic use, and provision for devastating civil remedies, including divestment or liquidated damages secured by bond, if necessary. This would prevent a company like Lenovo – owned by the Chinese government – from acquiring a U.S. company like IBM, which supplies IT equipment to the government and U.S. industry. In other words, Exon-Florio should be reformed to make it cost-prohibitive to compromise U.S. security or spy on the U.S., particularly through technical means, such as spyware or technical hardware inserted clandestinely into U.S. products. Exon-Florio should, in short, leverage a company's internal risk management proceedings to shift the burden of staying clear of espionage-related activity to the company, which is in the best position to avoid espionage-related activity in the first place.

investigations by such committee, and for other purposes; S.2380, 109th Cong. (2d Sess. 2006), To add the heads of certain Federal intelligence agencies to the Committee on Foreign Investment in the United States, to require enhanced notification to Congress and for other purposes.

98. Recall, Lenovo is owned by the Chinese government. See supra note 13.
2. Companies are permitted to submit voluntarily to review.\textsuperscript{99} Most do, because entering into such an acquisition transaction without review, only to have the government discover the transaction after the fact, investigate, and obtain a judicial divestment order, would be extremely costly and would represent a highly imprudent business practice.\textsuperscript{100} Additionally, transactions can be reviewed based on a referral by a CFIUS member with actual knowledge of the pending transaction.\textsuperscript{101} On the other hand, the process of discovering, investigating, and seeking judicial enforcement of Exon-Florio could take months or years; if such a transaction were structured for the express purpose of committing or enabling national security or economic espionage, a foreign power could reap the benefit of the transaction for that period of months or years before the divestment order would issue. \textit{This vulnerability augurs in favor of requiring mandatory reporting of all Exon-Florio-covered transactions and prescribing a specific criminal penalty for failing to comply.}

3. CFIUS also, by regulation, requires that review and investigation, if warranted, of the transaction, including presidential certification, must occur within 90 days of receipt of a perfected notice.\textsuperscript{102} This 90-day period includes a 30-day review period, a 45-day investigation period (if necessary), and a 15-day presidential action period.\textsuperscript{103}

a. The compressed timeline is designed to prevent the CFIUS review process from working as a distinctive to FDI. However, thorough investigation of a potential national security vulnerability in a complex business transaction might require more time than 90 days; moreover, the CFIUS consensus requirement, requiring that all members of CFIUS agree that investigation of a particular transaction is not warranted,\textsuperscript{104} rather than a more expedient majority or supermajority decision, demonstrates that the government is willing to defer to comprehensive security review rather than more efficient,

\begin{flushleft}
\textsuperscript{99} 31 C.F.R. § 800.
\textsuperscript{100} See, e.g., Lee & Perkins, \textit{supra} note 66.
\textsuperscript{101} See \textit{id}.
\textsuperscript{102} See \textit{id}.
\textsuperscript{103} See \textit{id}.
\textsuperscript{104} See \textit{id}.
\end{flushleft}
investment-friendly certification procedures. A reasonable compromise reform, then, might be to prescribe through legislation a revised, expanded, timeline for every case, to ensure a comprehensive review in every case. In the alternative, if such expansion of the timeline is deemed hostile to FDI, or is shown through studies or practice to result in an intolerable net decline in FDI, Exon-Florio could be revised to permit the President or the Secretary of the Treasury to extend the 90-day timeline in exceptionally complex cases in which more time would work to the material advantage of the government, to balance FDI-attractiveness against national security concerns. The CFIUS regulations prescribing this timeline were, of course, authored in 1991, before the ascendancy of new national security threats (the age of terror and emerging state-based threats), and at the end of an era of an old one (the Soviet empire). Changing times may merit changing standards: while expediency in review of most cases is an inherently good thing, flexibility in prescribed review timelines in exceptional circumstances is a necessary and appropriate guarantor of security. Query: whether such an extension of the investigation time really would work to discourage multimillion or even multibillion dollar corporate acquisitions; in other words, will companies really fail to invest in American companies over an additional 45-day delay in approval, or is the specter of decreasing FDI a red herring? The FDI impact of prescribing such flexibility should be studied empirically by the appropriate authority before changing the current standards, so that the appropriate decision can be reached on the balance between encouraging FDI and enhancing security. Moreover, the utility of the consensus requirement of CFIUS, which portends well for security concerns because it requires all members of CFIUS to agree that a transaction should go forward, should be studied as well, examining the balance of expediency and encouragement of investment against the guarantee of security that consensus approval provides.

b. Congress should also examine whether CFIUS' reluctance to initiate formal, 45-day investigations due in any part to apprehension that a thorough investigation cannot be completed within 45-days, thereby shading the decision on whether to engage in the investigation to begin with; if so, I would recommend that Congress adopt legislation permitting the
Secretary of the Treasury to grant up to two automatic extensions of 45 days each to complete the investigation; in the alternative, the entire 90 day period could be doubled or fractionally extended, to ensure time to conduct quality reviews.

4. Prescribing substantial civil penalties expressed in terms of percentage of net worth of the acquiring company or some other value expression that applies proportional disincentives to large and small business organizations, rather than in absolute terms of dollars, for companies who undertake transactions without submitting to the CFIUS review process, gambling that the government will not order divestiture once the train has left the station, or for companies found, after approval, to engage in or facilitate activity detrimental to national security, such as espionage.

5. In its analysis of the national security impact of business transactions involving foreign entities, such as the Dubai ports transaction or the Lenovo acquisition of IBM's personal computer division, which was also approved by CFIUS, CFIUS relies in part on recommendations and intelligence estimates to assess threats and vulnerabilities. In particular, CFIUS efforts are augmented by the Intelligence Community Acquisition Risk Center (CARC), a new organization that reports to the Director of National Intelligence tasked with conducting intelligence and counterintelligence risk assessments of certain commercial transactions referred to it by CFIUS. For example, CARC also provided a risk assessment on the Dubai Ports World deal early in 2006, advising that the transaction could proceed. Clearly, CARC and CFIUS are designed to work together to limit national security vulnerabilities from foreign investment, despite the political whirlwind that accompanied the Dubai ports agreement. Reform the CFIUS structure to incorporate intelligence estimates, instead of outsourcing them to the CARC — in other words, merge CARC into CFIUS, while retaining direct CARC connections to the intelligence community and DNI, for the purpose of ensuring the insulation of the CARC's intelligence analysis from political

105. See Kimmitt testimony, supra note 77.
106. Id.
pressures. There is no apparent reason why CFIUS and CARC should exist as separate entities; rather, they should be merged to gain synergies and accountability over the intelligence risk assessment process. Given the pervasive "fiefdom" characteristic of interagency politics in the U.S. Government, a merger would come laden with a complex set of subissues, but the most significant one is probably where the new, merged organization would reside. The Department of the Treasury's interests and expertise in monitoring the influence of foreign investment policy in the U.S. counsels that Treasury should maintain substantial influence on the process. However, the potential nexus between FDI and terrorism/espionage dictates that the organization should have robust DNI representation to inform CFIUS decisions. For example, DNI could be required to second to CFIUS/CARC a career intelligence professional, preferably of Senior Executive Service rank, as the deputy director or staff director of the new organization, along with hearty staff representation.

6. Install an equitably rotating chair, with Treasury serving as principal deputy during the periods that Treasury does not hold the chair, instead of relying on Treasury to chair CFIUS all the time. The GAO report identified the reluctance of Treasury to interpret "national security" with sufficient breadth to sweep in more transactions for review;\(^{108}\) in other words, Treasury leadership of CFIUS may represent a liability through cultural cautiousness. This may be because the Department of Treasury is impregnated with an "FDI first" cultural attitude, in much the same way that defense or intelligence community representatives might be infected with a "security first" presumption. By rotating the chair, a more balanced "investment/security" culture of practice should emerge, changing the culture of CFIUS gradually to cure this defect identified by the GAO report.

7. If rotating the chair is an insufficient measure to change the culture of cautiousness with regard to investigations, then Congress ought to more closely study the issue and mandate a shift in culture through legislation, perhaps by assigning a definition of "national security" in an amendment to Exon-Florio that opens the field of transactions that should be reviewed and investigated. The GAO report notes that Treasury, among other

\(^{108}\) See GAO Report, supra note 87 at 11.
agency members of CFIUS, define “threat to national security” as “risks associated with export-controlled technologies, classified contracts, and specific derogatory intelligence with respect to a foreign acquiring company,”\textsuperscript{109} noting that such a definition probably excludes review of transactions touching “critical infrastructure, defense supply, and defense technological superiority.”\textsuperscript{110} Under the present standard of practice, such a narrow definition might also exclude from routine review transactions such as the Lenovo acquisition of the IBM subsidiary (although a 30-day review of that transaction was, in fact, taken). One set of commentators notes that Senator Inhofe, a frequent critic of CFIUS, has suggested that the concept of national security should be interpreted to include economic and energy security, in addition to more traditional interpretations.\textsuperscript{111} Congress may provide minimum standards that must be considered and weave “aggressive review” intent language into the legislative history of the amendment, then leave it to the agency to determine the remainder of the content of “national security” for the purpose of CFIUS review determinations. Congress could also sunset the amendment, which would provide an automatic occasion for reviewing CFIUS’s performance in effecting the new balance between security and FDI.

8. Congress should consider shifting the burden of proof and concurrence quorum required to avoid convening an investigation. Currently, CFIUS convenes a “45-day investigation” only if all members agree that one should be conducted.\textsuperscript{112} Congress should consider mandating 45-day investigations in all cases, permitting CFIUS to vote by consensus to invoke an exception to avoid convening an investigation. Alternatively, rather than shifting the presumption of “no investigation,” Congress could mandate a quorum smaller than consensus to convene an investigation, such as a majority or 2/3 vote of the members.

9. Through amendment to Exon-Florio, explicitly and clearly empower the president to seek judicial divestment or dissolution orders for corporate transactions previously reviewed and certified

\textsuperscript{109} Id. (citing GAO Report, supra note 87 at 39-46).
\textsuperscript{110} Id.
\textsuperscript{111} See Lee & Perkins, supra note 66.
\textsuperscript{112} Id.
by CFIUS (no 45-day investigation) or the president (in the case of a transaction on which the president is required to act), or for corporate transactions not previously examined under the statute, where one or more of the business organizations involved in the transaction conducts espionage-related activities. In other words, amend Exon-Florio to reach the facially-innocent transaction that later reveals itself to be an instrumentality of espionage, and provide a divestment/dissolution remedy to deter through economic prohibition, by making it too expensive for companies to spy or enable spying through design or neglect.

10. Finally, reform CFIUS or a subsidiary entity to incorporate a technical review mechanism—perhaps establishment of a lower-level working group, etc.—to conduct technical review of products purchased by the U.S. government with foreign made, originated, assembled, or distributed products or components, including a legislative provision to prescribe substantial civil penalties for failure to disclose such products or components. The newly merged CFIUS/CARC working group entity should be resourced to conduct technical exploitation of products acquired from abroad for U.S. government use, including reverse-engineering of prioritized representative samples of purchased equipment.

V. THE DEFENSE TECHNOLOGY SECURITY ADMINISTRATION'S FUNCTION IN COUNTERESPIONAGE AND TECHNOLOGY SECURITY

Finally, within the Department of Defense, the Defense Technology Security Administration (DTSA) is tasked by the Secretary of Defense with reviewing and coordinating the issuance of thousands of export licenses each year for U.S. technology pending sale to other countries. The DoD Manual mandating procedures for information security in procurement, the DoD National Industrial Security Program Operating Manual, "provides baseline standards for the protection of classified information released or disclosed to industry in connection with classified contracts"—in other words, it is designed to prevent

the release of classified information to industry and, thus, making it vulnerable to disclosure to foreign powers.

There does not, however, appear to be an agency in DoD with explicit responsibility for reviewing products being purchased by the U.S. from abroad, particularly information systems. One worthwhile reform to the DTSA mission would be to task it with developing and implementing procedures to ensure the testing/reverse-engineering of a representative sampling of information technology gear imported from other countries for the presence of bugs, listening devices, or programming code designed to capture and transmit automatically data to a receiving agent of a foreign power. If this function were to be exercised comprehensively by CFIUS/CARC, then there would be no need for DoD to exercise the function independently; but if CFIUS/CARC cannot provide a comprehensive technical security review process at the DNI level, then DoD should be able to guard its own secrets from foreign exploitation through an expanded mission for DTSA.

VI. CONCLUSION

In conclusion, technically-driven parasite programs and equipment, engineered to "ride along" on commercial host products acquired from abroad or from domestic sources controlled by foreign entities from abroad, represent a substantial espionage threat to U.S. entities, particularly the government. The methods of attacking this threat could be myriad and varied; the minor modification and use of RICO and focused efforts by a reformed and streamlined CFIUS could go a long way toward ensuring that those items of electronic equipment acquired for the conduct of business and government work do not silently spy on U.S. policymakers and implementers by passively gathering information and data and transmitting it to foreign power receivers. The government can leverage the power of industry to self-police their manufacturing, assembly, and distribution processes to keep them pure from the corrupting influence of foreign intelligence collection. Finally, CFIUS reform has implications above and beyond simply limiting technically-based espionage. CFIUS is the primary means by which the U.S.

2, 2007).
government screens foreign influence through business acquisition in the U.S. generally. Improvements in its efficiency and effectiveness are vital to preserving U.S. national security, particularly limiting espionage and counterterrorism vulnerabilities.